Identity Theft: A Guide For Victims

This sheet contains important information for you if:

- Someone has used your personal identifying information (your name, address, telephone number, social security number, driver's license number, etc.) without your consent for an unlawful purpose.
- Your wallet, purse or mail were recently stolen containing credit cards or applications, blank or completed checks, your driver's license, social security number, work or school ID, passport, etc.

Your personal information can be used by thieves to apply for credit, to create and use counterfeit checks or credit cards, to establish new phone service, obtain medical care, or to purchase items on credit by phone or mail. This may go on for months or years without you even knowing it! This sheet contains important information to reduce the risk and damage to you of identity theft.

Although you are not responsible for monetary losses that result from identity theft, you should protect yourself from being further victimized and act immediately to minimize the damage to your credit. Notify the following agencies and financial institutions and keep a record of your conversations and copies of all letters and documents.

Law Enforcement: Report identity theft crimes immediately to your local police department and to the FTC at 877-438-4338 or **www.ftc.gov**. Penal Code 530.6 requires your local police department to take your report, regardless where the identity theft occurred, and forward it to the law enforcement agencies located where the checks or credit cards were used, or where the fraudulent credit applications were presented. When possible prepare a typed statement of what happened and provide it to officers, along with documentation of the fraudulent accounts and charges, including the city & state where the fraud occurred. The theft of your wallet, purse, or mail is a separate crime from the fraudulent use of your identity, often involving different perpetrators. If you have not already done so you should make a police report for the theft – separate from the fraudulent use of your identity. Record the police report number(s) you're given and provide them to your creditors. Although the police will take your report, it will be up to you to make all the necessary contacts to protect yourself from further loss and to restore your credit. Lack of evidence often prevents police from making arrests in every case, but your timely report is valuable in any case.

Credit Bureaus: Call all three credit reporting companies. Report the theft and fraudulent use of your checks, credit cards, ID, or social security number. Ask that your account be flagged for fraud. Also, add a statement to your report, up to 100 words, "My identity has been used to apply for credit fraudulently. Contact me at (home or work telephone #) to verify all applications." Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. **California Civil Code 1785.15.3(b)** now entitles identity theft victims to a free copy of their credit report every month for 12 months. **Civil Code 1785.11.2(m)** allows you to put a freeze on your credit report free of charge, to prevent new accounts being opened in your name.

If fraudulent accounts have been opened in your name, ask the credit bureaus for names and phone numbers of credit grantors. Send each credit bureau a copy of your police report, and ask them to block the fraudulent information immediately - **Cal. Civil Code 1785.16(k)** requires them to do so. Ask the credit bureaus to notify those who have received your credit report recently, to alert them to the disputed and erroneous information.

Credit Reporting Bureaus

Equifax **www.equifax.com** P.O. Box 740241, Atlanta, GA 30374-0241 To report fraud call: 800-525-6285 For a credit report: 800-685-1 111.	Experian *(formerly TRW)* **www. experian. com**. P.O. Box 1017, Allen, TX 75013 To report fraud call: 888-397-3742 For a credit report: 800-682-7654.	Trans Union **www.tuc.com** P.O. Box *390,* Springfield, PA 19064 To report fraud call: 800-680-7289 For a credit report: 800-916-8800.

Creditors: Contact all creditors and merchants with whom your name has been used fraudulently by phone and in writing. Provide fraud affidavits or written statements and supporting documentation as requested. You can download a form from the Federal Trade Commission website to use in notifying creditors at **www.consumer.gov/idtheft**. Close old accounts and get replacement cards with new account numbers for accounts that have been used fraudulently. Carefully monitor your mail and credit card bills for evidence of new fraudulent activity and report it. For information about how to obtain a copy of a fraudulent application made in your name contact the California Department of Consumer Affairs at 800-952-5210 or visit **www.privacyprotection.ca.gov**.

Cal. Penal Code 530.8 requires creditors to give you the personal information used to open a fraudulent account in your name, and all the transactions conducted on that account, once you give them a copy of your police report.

Stolen checks or counterfeit checks: If you have had checks stolen or counterfeited, or bank accounts set up fraudulently, report it the police and to every one of the listed check verification companies. Banks do not automatically send them fraud reports and they do not share data with each other. Cancel all bank accounts affected by fraud, and obtain new account numbers. Stop-payments are *not effective* because they only last 90 days – and they cost you money. Also, stolen account numbers can be used to print new checks on personal computers with check-writing software, and to make fraudulent automated transfers.

Check Verification Services *(Call all of them)*

• CheckRite: 800-766-2748	• Int'l Check Services: 800-526-5380
• Chexsystems: 800-428-9623	• SCAN: 800-262-7771
• CrossCheck Inc.: 800-843-0760	• TeleCheck: 800-710-9898
• Equifax: 800-437-5120	

ATM Cards: If your ATM card has been stolen or compromised get a new card, account number and PIN. Do not use your old PIN. When creating a PIN don't use common numbers like the last four digits of your Social Security number or your birth date.

Driver's License: If someone is using your driver license information as identification on bad checks or for traffic violations, report this to police and to Investigators at the nearest office of the Department of Motor Vehicles (DMV). Ask if any other licenses were issued in your name and put a fraud alert on your DMV record. You may ask for a new drivers license number.

- California Department of Motor Vehicles (DMV) fraud unit: 866-658-5758, email dlfraud@dmv.gov, or **www.dmv.ca.gov**

Mail Theft or fraudulent change of address:
Make a report with the local Postal Inspector if you suspect someone has stolen your mail, filed a change of your address or has used the mail to commit credit or bank fraud. If you find out where fraudulent credit cards in your name were sent, notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

- U.S. Postal Inspection Service: 415-778-5800, **www. usps.gov/websites/departinspect**

Social Security Number misuse: Call the Social Security Administration to report fraudulent use of your Social Security number. Be aware the SSA will only issue you a new number if you fit their fraud victim criteria. You should order a copy of your Earnings and Benefits Statement and check it for accuracy.

- Social Security Administration: To report fraud: 800-269-0271.
- To order your Earnings and Benefits Statement: 800-772-1213

Passports: If your passport has been stolen notify the passport office in writing.

- Passport Agency 95 Hawthorne St., ~ Floor, San Francisco, CA 94105

Utilities & Phone Service: If someone has ordered service in your name cancel the account and open a new one. Provide a password that must be used any time the account is changed. If you are having trouble with falsified accounts contact the State Public Utilities Commission.

Internet Fraud: Report suspected criminal or civil fraud committed over the internet to the FBI at **www.ifccfbi.gov**

Traffic Citations, Suspensions, or Revocations Issued in Your Name

Make a police report of identity theft with your local law enforcement agency, and submit to the issuing court your right thumbprint and a statement under penalty of perjury, that you are not the person to whom the citation or warrant was issued, per Vehicle Code 40500(e). Request a finding of factual innocence, as authorized in Penal Code 530.6. For criminal warrants, you may have to request a hearing in the county where the warrant was issued.

Your Consumer Rights

You are not required to pay any bill or portion of a bill that is a result of identity theft. Any payment you do make could be used to prove your liability for the debt. You are not required to cover any checks that were written or cashed fraudulently. Your credit rating should not be permanently affected and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. You may wish to consult with an attorney.
For more information about-privacy rights and identity theft, including links to many other government agencies, contact the CDSA Office of Privacy Protection. They provide downloadable forms in several different languages.
Cal. Dept. of Consumer Affairs, Office of Privacy Protection; tel. 800-952-5210, **www.privacyprotection.ca.gov**

How to Protect Yourself

- Buy a shredder and use it before you discard or recycle any papers containing your name or personal information.
- Shred all junk mail, especially pre-approved credit card offers or convenience checks – a common source of fraud.
- Never carry your social security number or passport unless necessary. Only carry credit cards you plan to use.
- Photocopy the contents your wallet and keep the copies in a safe place, if needed later to make a police report.
- Get a copy of your credit report every year from all three Credit Reporting Bureaus, to check for new fraudulent accounts.
- Check your bank and credit card statements every month for fraudulent charges, additional signers, or address changes.
- Unless your mailbox is secure, mail check payments at the post office and pick up new checks at the bank to avoid theft.
- Don't give identifying information over the phone or internet to anyone you didn't call or don't know personally.
- Never leave your checkbook, purse or wallet in a vehicle, an office desk drawer, on a chair, or in shopping cart.
- Beware of pickpockets when in crowds or taking public transportation, and carry your wallet or purse in front of your body.
- Don't use your mother's maiden name as a password. Family names are available over the internet.